2011 DoD BIOMETRICS COLLABORATION FORUM

Biometric Equities for Identity & Privilege Management Working Group (IPvMWG) Roadmap

BIMA BIOMETRICS IDENTITY MANAGEMENT AGENCY

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **JAN 2011**	2. REPORT TYPE	3. DATES COVERED **00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE **Biometric Equities for Identity & Privilege Management Working Group (IPvMWG) Roadmap**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Research and Engineering,Biometrics Identity Management Agency (BIMA),Washington,DC,20301**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

presented at the 2011 DoD Biometrics Collaboration Forum held 25-27 Jan.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**30**	

Biometric Equities for Identity & Privilege Management Working Group (IPvMWG) Roadmap

- BBFF
- IPMSCG Overview
- IPvMWG Overview
- IPvM CONOPS Development
- Biometric Equities

Biometrics-enabled Business Function Framework (BBFF)

- The Biometrics-Enabled Business Functions Framework (BBFF) is intended to facilitate evaluation and integration of biometrics technologies into DoD business processes to increase effectiveness, efficiencies and accuracy while complying with DoD privacy, security, and information exchange policies/requirements.

- The BBFF has three critical perspectives:
  - **Strategic** – Authorities (Identity, Access Control & S&T)
  - **Operational** – Policy & Acquisition (implementing solutions)
  - **Technical** – biometrics technologies & biometrics solutions / systems

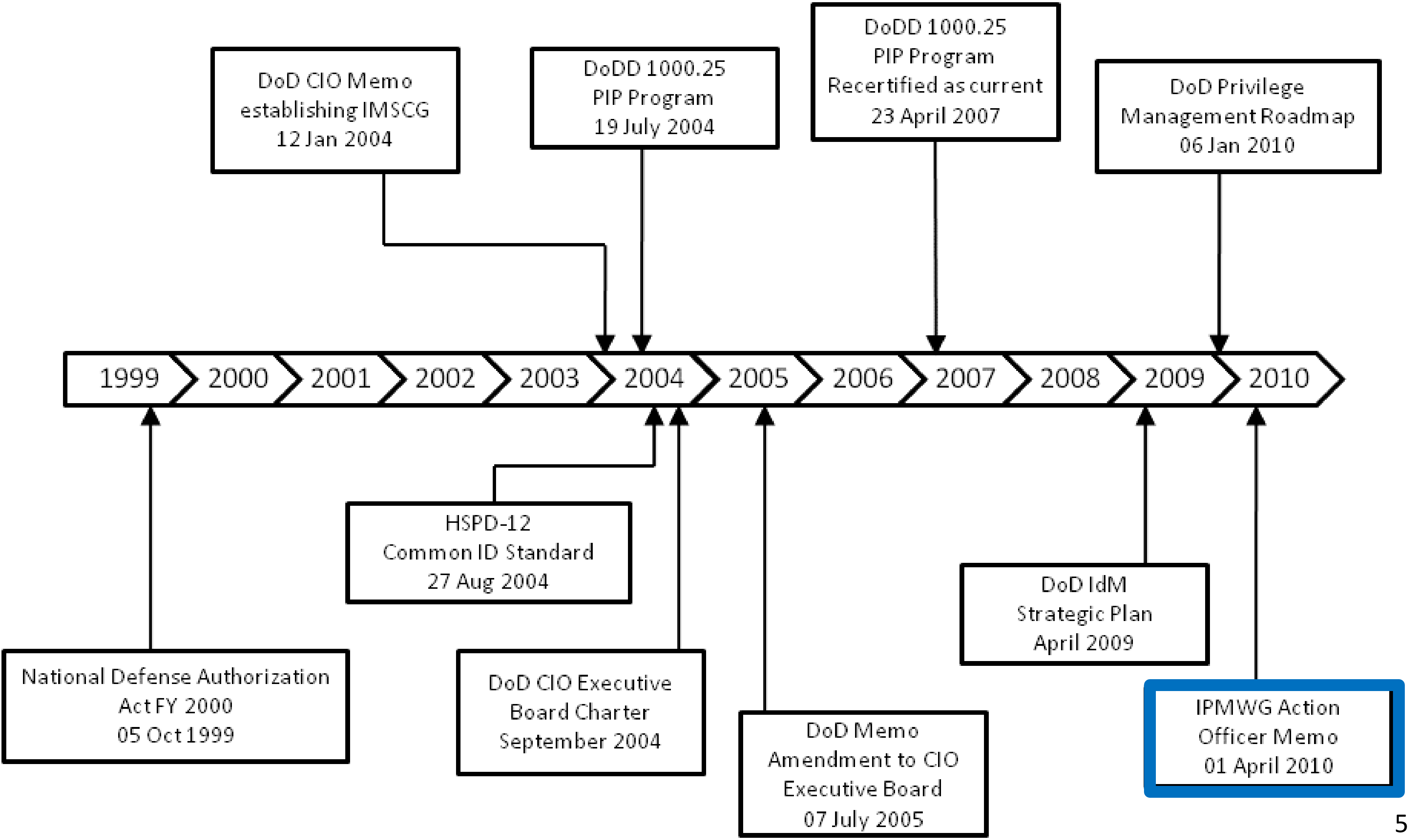
- The Friendly Biometrics BCF2011 Track has a focus on collecting community feedback to enable the development of the BBFF.

Identity Protection & Management Senior Coordinating Group (IPMSCG) Overview

- 05 Oct 99, Public Law 106-65 - Congress directed a Senior Coordinating Group for Smart Card Technology w/ DoD CIO oversight
- 0 Nov 99, Deputy Secretary of Defense Memo, Smart Card Adoption & Implementation - destablished the Smart Card Senior Steering Group and defined the Smart Card Senior Coordinating Group (SCSCG) and the Smart Card Configuration Management Control Board (SCCMCB)
- 31 Aug 02, DoDD 8190.03, Smart Card Technology – unified the role of the SCCMCB with the SCSCG
- 12 Jan 04, DoD CIO Memo established the Identity Management Senior Coordinating Group (IMSCG) in place of the SCSCG and outlined the Biometric Management Office to provide executive secretariat support along w/ CAC and PKI offices.
- 19 Jul 04, Certified Current 23 Apr 07, DoDD 1000.25 Personnel Identity Protection (PIP) Program rename IMSCG as the Identity Protection Management Senior Coordinating Group (IPMSCG) and establish Joint oversight between USD (P&R) and DoD CIO.

- **IPMSCG is the nexus for friendly forces Identity Protection & Management (IPM)**
- **Biometrics is a recognized critical enabler for friendly forces IPM challenges**

DoD Identity Management (IdM) Implementation Guidance



DoD CIO Memo establishing IMSCG 12 Jan 2004

DoDD 1000.25 PIP Program 19 July 2004

DoDD 1000.25 PIP Program Recertified as current 23 April 2007

DoD Privilege Management Roadmap 06 Jan 2010

National Defense Authorization Act FY 2000 05 Oct 1999

HSPD-12 Common ID Standard 27 Aug 2004

DoD CIO Executive Board Charter September 2004

DoD Memo Amendment to CIO Executive Board 07 July 2005

DoD IdM Strategic Plan April 2009

IPMWG Action Officer Memo 01 April 2010

IPvMWG Responsibilities

- Lead the implementation of the DoD Identity Management Strategic Plan and DoD Privilege Management Roadmap
- Develop IPvM Roadmap & Milestones
- Transition IPMSCG approved Identity and Privilege Management (IPvM) recommendations into implementable activities
- Synchronize and coordinate IPvM efforts across the DoD and with federal partners
- Participants:
  - DoD Components
  - Military services
  - DoD Agencies

IPvMWG Progress Update

DoD IdM Strategic Plan

Signed by
DoD CIO
USD (P&R)
USD (I)
USD (AT&L)
USD (P)
Apr 2009

Department of Defense
Privilege Management Roadmap

DoD PvM Roadmap

DoD Identity Management Strategic Plan

April 2009

Signed by Dep CIO
Jan 2010

DoD Enterprise-wide IPvM Recommendations

UNCLASSIFIED

DoD Enterprise-wide

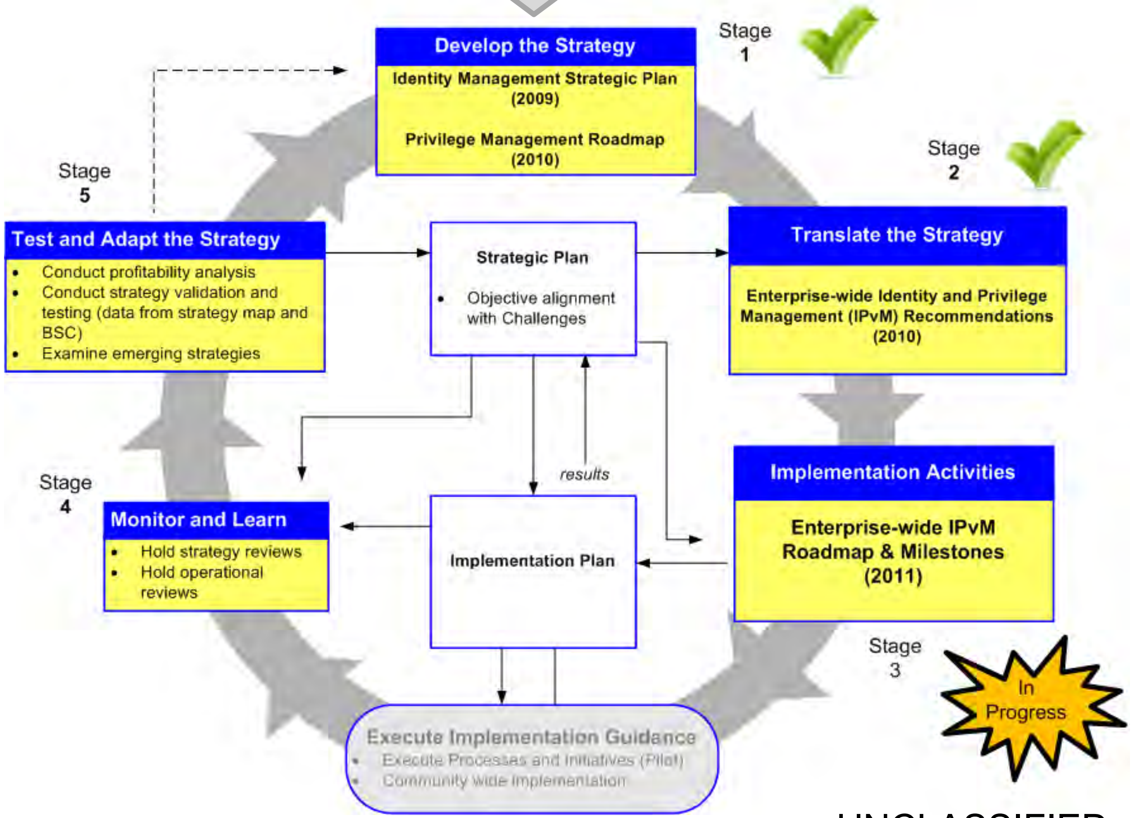
Identity & Privilege Management (IPvM)

Recommendations

22 November 2010

UNCLASSIFIED

Approved by
IPMSCG chair
September 2010


Develop the Strategy

Stage 1

Identity Management Strategic Plan (2009)

Privilege Management Roadmap (2010)

Stage 2

Translate the Strategy

Enterprise-wide Identity and Privilege Management (IPvM) Recommendations (2010)

Implementation Activities

Enterprise-wide IPvM Roadmap & Milestones (2011)

Stage 3

In Progress

Execute Implementation Guidance
- Execute Processes and Initiatives (Pilot)
- Community wide implementation

Stage 4

Monitor and Learn
- Hold strategy reviews
- Hold operational reviews

Stage 5

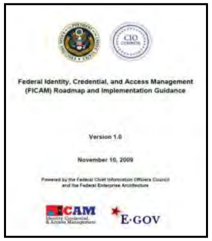
Test and Adapt the Strategy
- Conduct profitability analysis
- Conduct strategy validation and testing (data from strategy map and BSC)
- Examine emerging strategies

Strategic Plan
- Objective alignment with Challenges

results

Implementation Plan

+


Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance

Version 1.0

November 10, 2009

Powered by the Federal Chief Information Officers Council and the Federal Enterprise Architecture

FICAM Federal Identity, Credential, & Access Management

E-GOV

FICAM Roadmap & Implementation Guide (draft) November, 2009

=

Draft Working Papers

DoD Enterprise-wide Identity & Privilege Management (IPvM)
Roadmap & Milestones
Version 0.1
2011
NOT APPROVED FOR PUBLIC RELEASE

LEGEND FOR OUTLINE
YELLOW – NOTES ON WHAT TO INSERT
🟥 – ORGANIZATION RESPONSIBLE

DoD IPvM Roadmap (draft)

Implements to Support

DOD
IT CONSOLIDATION
ROADMAP

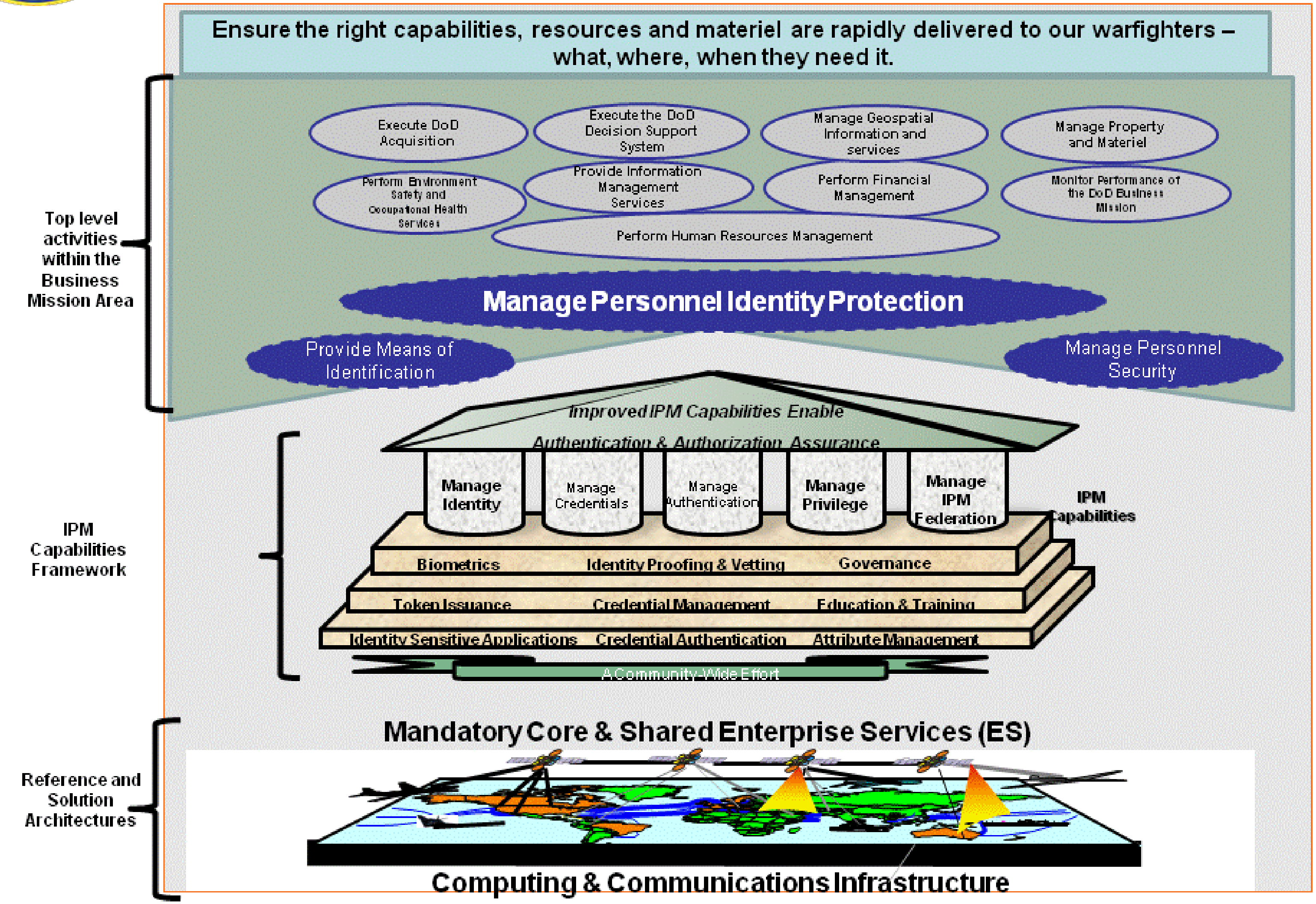
DoD IT Consolidation Roadmap (draft)

UNCLASSIFIED

IPvM Strategic Plan Goals

- Goal 1: Unity of Purpose for Effective Governance and Employment of IPvM
- Goal 2: Institutionalize the DoD IPvM capability and culture across the Department
- Goal 3: Build, deploy, operate and maintain a reliable, interoperable and secure IPvM capability

Identity & Privilege Management (IPvM) in the Business Enterprise Architecture (BEA)



Ensure the right capabilities, resources and materiel are rapidly delivered to our warfighters – what, where, when they need it.

Top level activities within the Business Mission Area

Execute DoD Acquisition

Execute the DoD Decision Support System

Manage Geospatial Information and services

Manage Property and Materiel

Perform Environment Safety and Occupational Health Services

Provide Information Management Services

Perform Financial Management

Monitor Performance of the DoD Business Mission

Perform Human Resources Management

Manage Personnel Identity Protection

Provide Means of Identification

Manage Personnel Security

IPM Capabilities Framework

Improved IPM Capabilities Enable Authentication & Authorization Assurance

Manage Identity

Manage Credentials

Manage Authentication

Manage Privilege

Manage IPM Federation

IPM Capabilities

Biometrics

Identity Proofing & Vetting

Governance

Token Issuance

Credential Management

Education & Training

Identity Sensitive Applications

Credential Authentication

Attribute Management

A Community-Wide Effort

Reference and Solution Architectures

Mandatory Core & Shared Enterprise Services (ES)

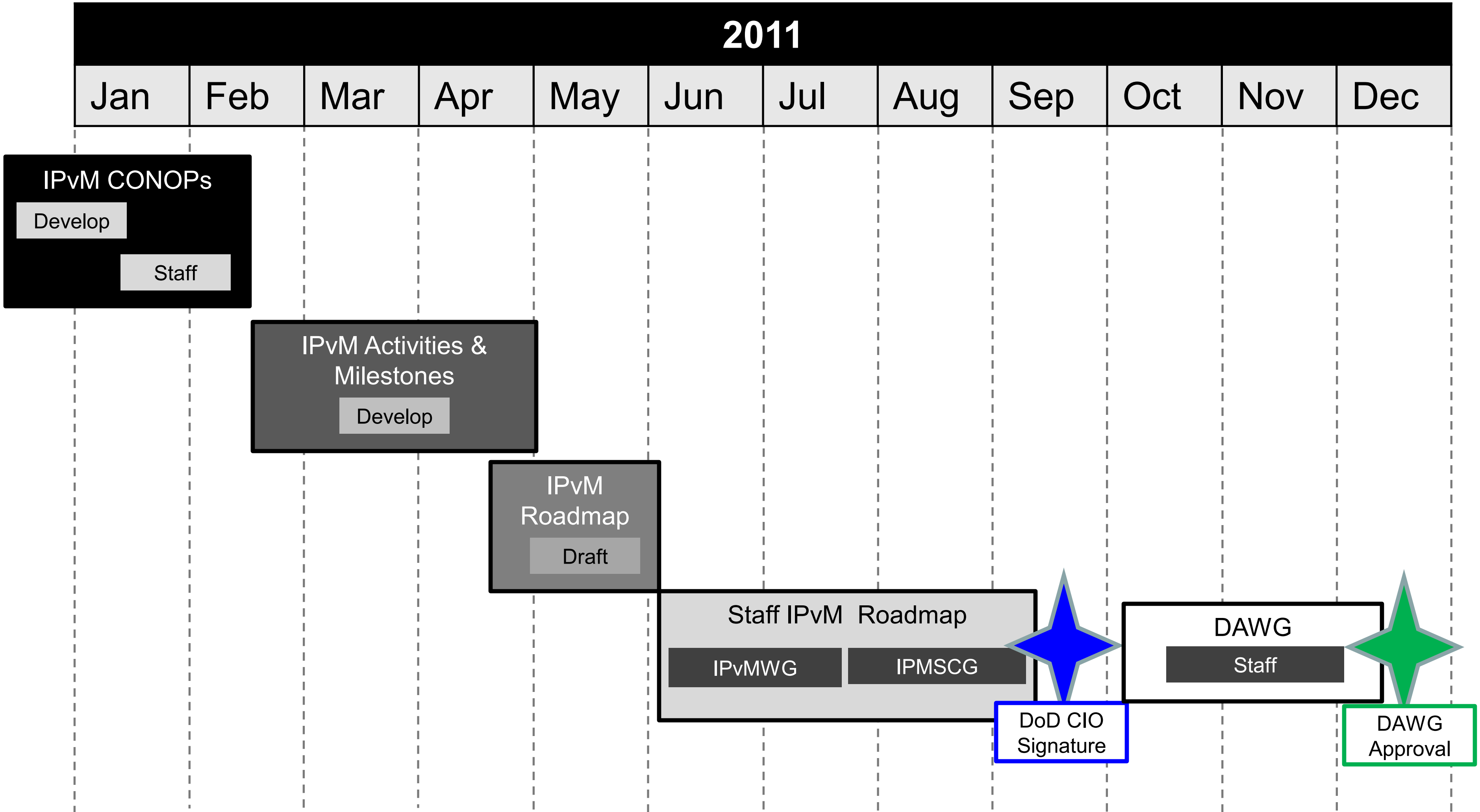
Computing & Communications Infrastructure

IPvM "Cornerstone" Recommendations

1. **Execute IPvM performance management**
   - Develop an IPvM Roadmap & Plan of Action & Milestones (POA&M) and measure progress of the integration of interoperable IPvM capabilities across DoD Mission Areas
   - Utilize existing governance structures (IPMSCG, DAWG, etc.)
2. **IPvM Outreach to Functionals across DoD and beyond:**
   - Work with functional area architectures advocating priorities important to IPvM to institutionalize integrated & interoperable IPvM IT Investment Review Board decision-making across the DoD Business Enterprise
   - Promote the interdependencies between mission areas regarding IPvM capabilities
   - Coordinate and synchronize activities with ICAMSC and AASC
   - Enhance cyber security through DoD Enterprise-wide Identity & Privilege Management
3. **Organize, update, amplify existing architectures and embrace federated architectures**
   - Integrate IPvM capabilities into DoD Mission Areas (BMA,WMA,IMA)
   - Force IPvM compliance through funding constraints
     - Insert IPvM criteria into the USD P&R Human Resources Management (HRM) Enterprise Architecture (EA) and ultimately into the Business Enterprise Architecture (BEA)

Authority: IPMSCG Chair approved the cornerstone recommendations and assigned the IPvMWG to execute the development of the Roadmap & Milestones

Tentative IPvM Roadmap Timeline



2011

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

IPvM CONOPs

Develop

Staff

IPvM Activities & Milestones

Develop

IPvM Roadmap

Draft

Staff IPvM Roadmap

IPvMWG

IPMSCG

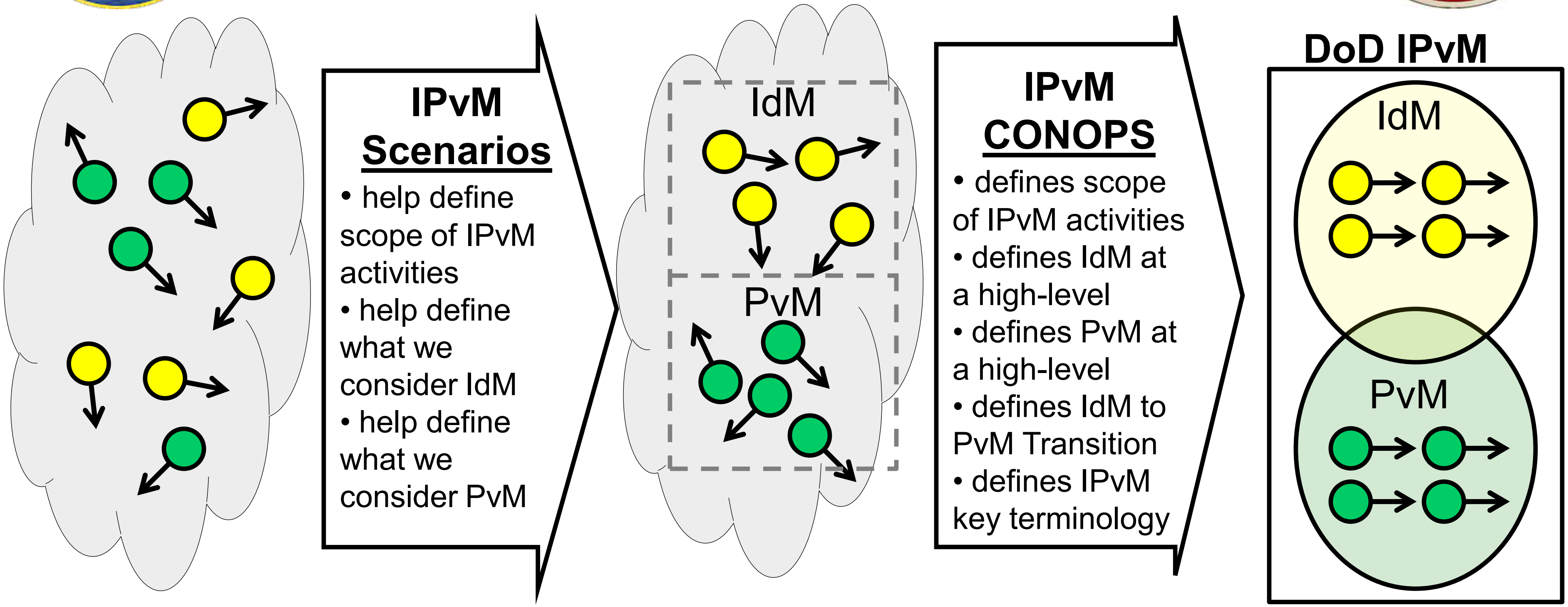
DoD CIO Signature

DAWG

Staff

DAWG Approval

Stages of IPvM CONOPS Development



IPvM <u>Scenarios</u>

- help define scope of IPvM activities
- help define what we consider IdM
- help define what we consider PvM

<u>IPvM CONOPS</u>

- defines scope of IPvM activities
- defines IdM at a high-level
- defines PvM at a high-level
- defines IdM to PvM Transition
- defines IPvM key terminology

Current State – IPvM is not a recognized, managed attribute across the DoD Enterprise

IPvM Scenario Development will help define scope of DoD Enterprise IPvM Road Map impacts and what are existing attributes of Identity Management (IdM) & Privilege Management (PvM).

IPvM CONOPS clearly defines the agreed upon and desired end-state of the IPvM Roadmap & Milestones to focus sub-working group activities.

Steps towards IPvM CONOPS

- ✓ Submit Stakeholder Scenarios
- ✓ Validate Identities of Interest
- ✓ Develop Conceptual Model / Cartoon
- ✓ Identify potential IPvM Use Cases
- Identify notional integration of IPvM Management & Technical Frameworks
- Identify IPvM National Security / Joint War fighting Capability Objectives
- Distinguish between Enterprise and Local IPvM Services

IPvM Identities of Interest

DoD IdM Strategic Plan identities:

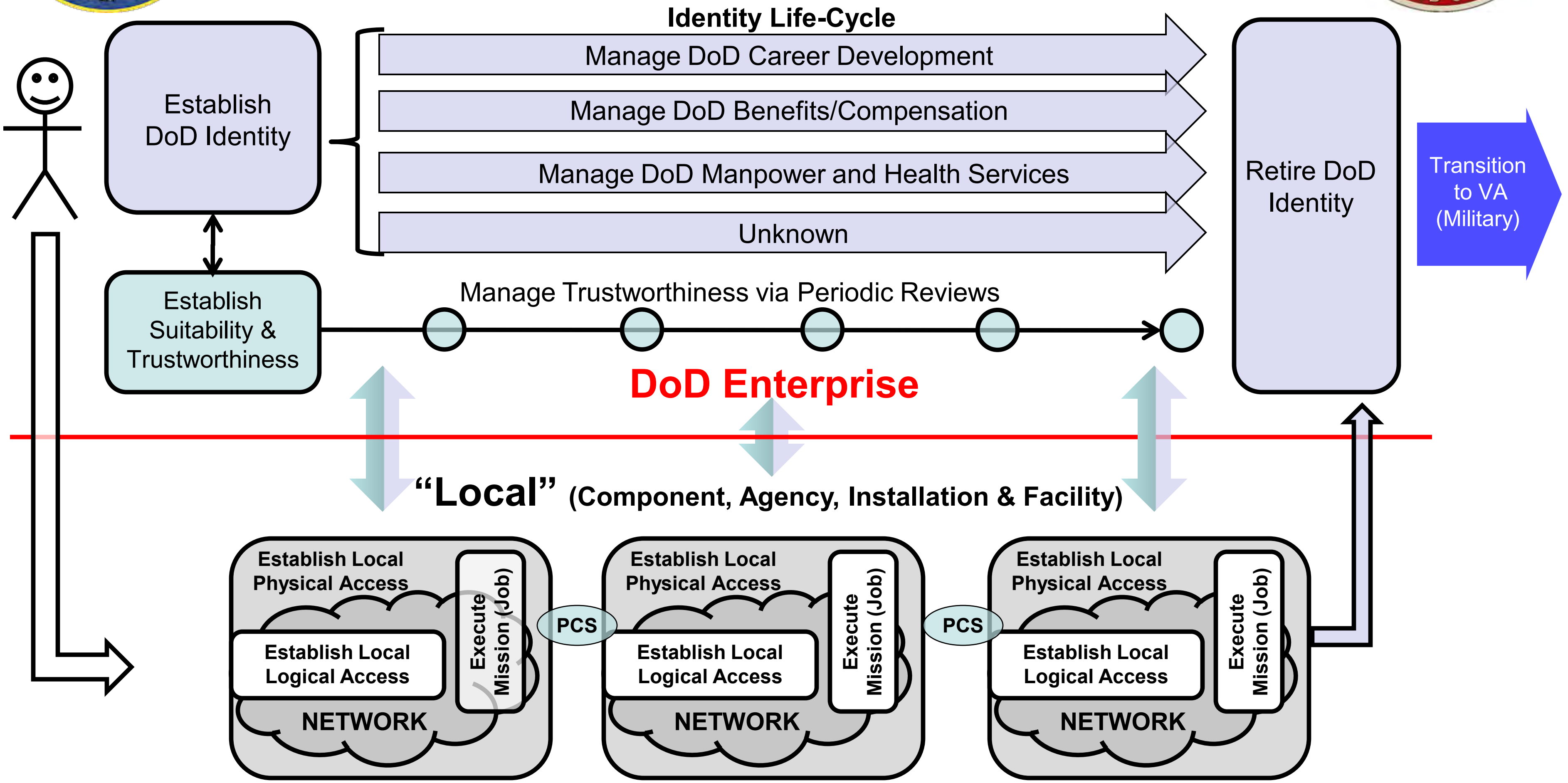
- Individuals and Non-Person Entities (NPEs)
  - **Blue / Friendly Forces** - e.g., DoD Civilian, Military, Contractors, Dependents, Vendors, Federal, State, Local, Tribal
  - **Red / Adversary** - e.g., Nation State, Asymmetric
  - **Gray / Neutral** - e.g., US Citizen, Coalition, Not-Adversary but Foreign, Industry, NGOs

These are the IPvM identities of interest to be covered in the Roadmap.

Draft IPvM Scenario Themes

Draft IPvM Scenario Themes
Hiring
Physical Access
Logical Access
Retirement
Financial Transactions
Forensics (red)
Raid (capture/kill)
Media Exploitation
Boarding at Sea
Humanitarian Assistance/Disaster Relief (HADR)

Draft IPvM Conceptual "Cartoon" DoD Military and Civilian



Identity Life-Cycle
Establish DoD Identity
Manage DoD Career Development
Manage DoD Benefits/Compensation
Manage DoD Manpower and Health Services
Unknown
Retire DoD Identity
Transition to VA (Military)
Establish Suitability & Trustworthiness
Manage Trustworthiness via Periodic Reviews
DoD Enterprise
"Local" (Component, Agency, Installation & Facility)
Establish Local Physical Access
Establish Local Logical Access
Execute Mission (Job)
NETWORK
PCS
Establish Local Physical Access
Establish Local Logical Access
Execute Mission (Job)
NETWORK
PCS
Establish Local Physical Access
Establish Local Logical Access
Execute Mission (Job)
NETWORK

USD Personnel & Readiness (P&R)
USD Intelligence (I)
Local commander/resource owner
Veterans Affairs (VA)

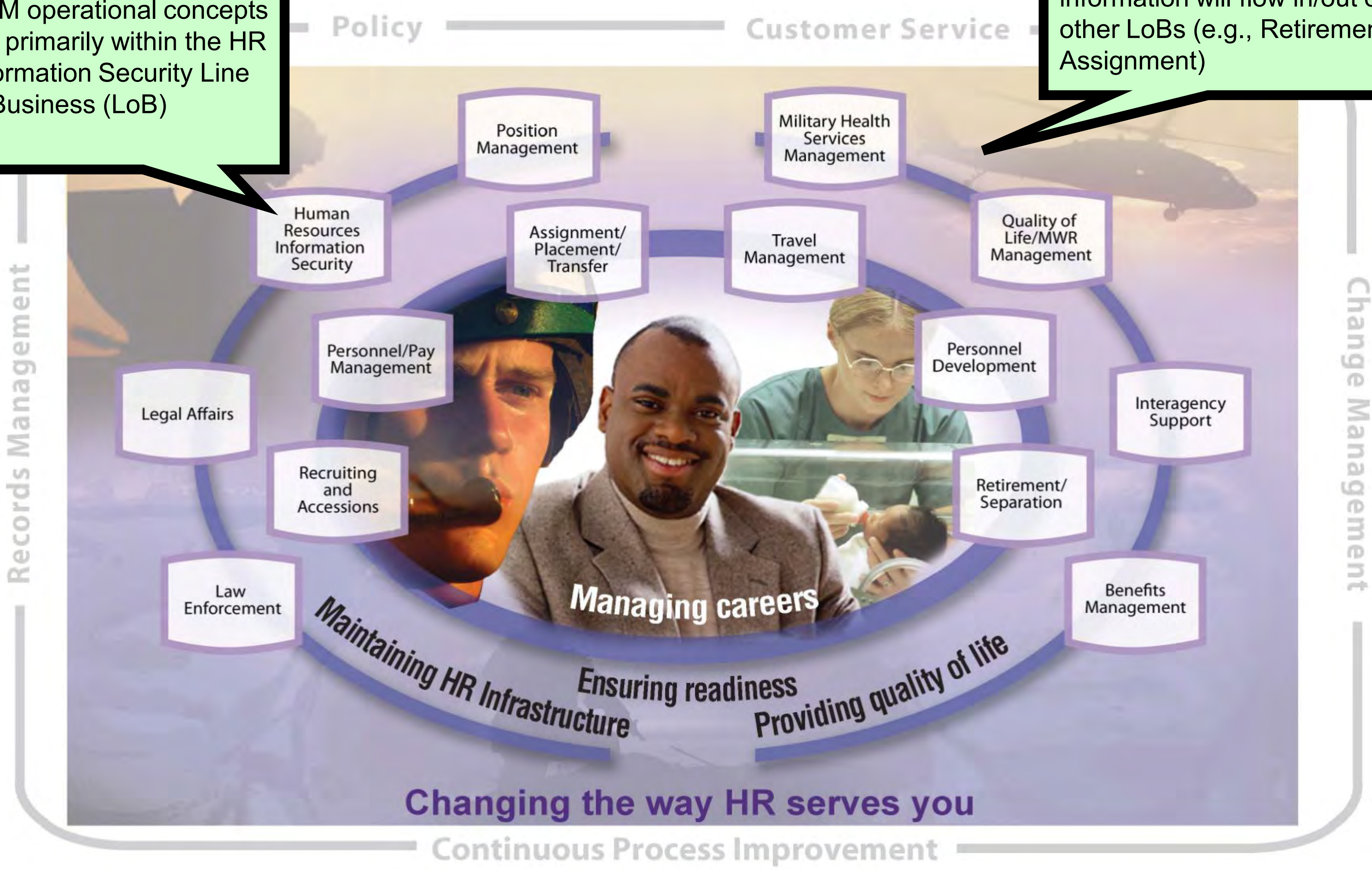
Terminology purposely abstracted up to very generic language & Concepts
IPvMWG will mature this "Cartoon" to a Model

UNCLASSIFIED

Human Resource Management (HRM) High-Level Operational Concept Graphic (OV-1)

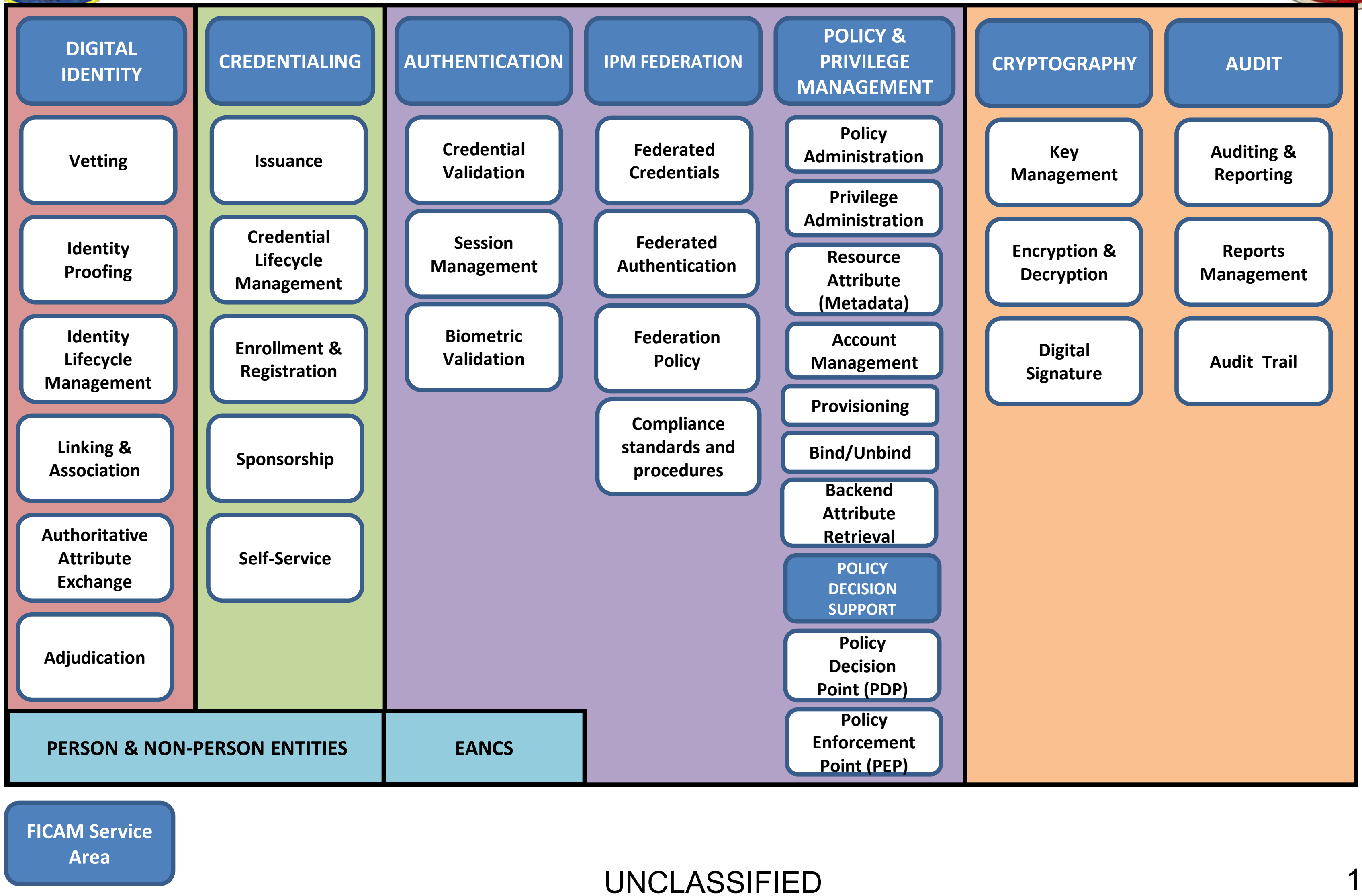
IPvM operational concepts are primarily within the HR Information Security Line of Business (LoB)

Identity and Privilege information will flow in/out of other LoBs (e.g., Retirement, Assignment)


Policy
Customer Service
Records Management
Change Management
Position Management
Military Health Services Management
Human Resources Information Security
Assignment/ Placement/ Transfer
Travel Management
Quality of Life/MWR Management
Personnel/Pay Management
Personnel Development
Legal Affairs
Interagency Support
Recruiting and Accessions
Retirement/ Separation
Law Enforcement
Benefits Management
Managing careers
Maintaining HR Infrastructure
Ensuring readiness
Providing quality of life
Changing the way HR serves you
Continuous Process Improvement

UNCLASSIFIED

Friendly / Blue : Draft DoD ICAM Framework



DIGITAL IDENTITY
- Vetting
- Identity Proofing
- Identity Lifecycle Management
- Linking & Association
- Authoritative Attribute Exchange
- Adjudication

CREDENTIALING
- Issuance
- Credential Lifecycle Management
- Enrollment & Registration
- Sponsorship
- Self-Service

AUTHENTICATION
- Credential Validation
- Session Management
- Biometric Validation

IPM FEDERATION
- Federated Credentials
- Federated Authentication
- Federation Policy
- Compliance standards and procedures

POLICY & PRIVILEGE MANAGEMENT
- Policy Administration
- Privilege Administration
- Resource Attribute (Metadata)
- Account Management
- Provisioning
- Bind/Unbind
- Backend Attribute Retrieval

POLICY DECISION SUPPORT
- Policy Decision Point (PDP)
- Policy Enforcement Point (PEP)

CRYPTOGRAPHY
- Key Management
- Encryption & Decryption
- Digital Signature

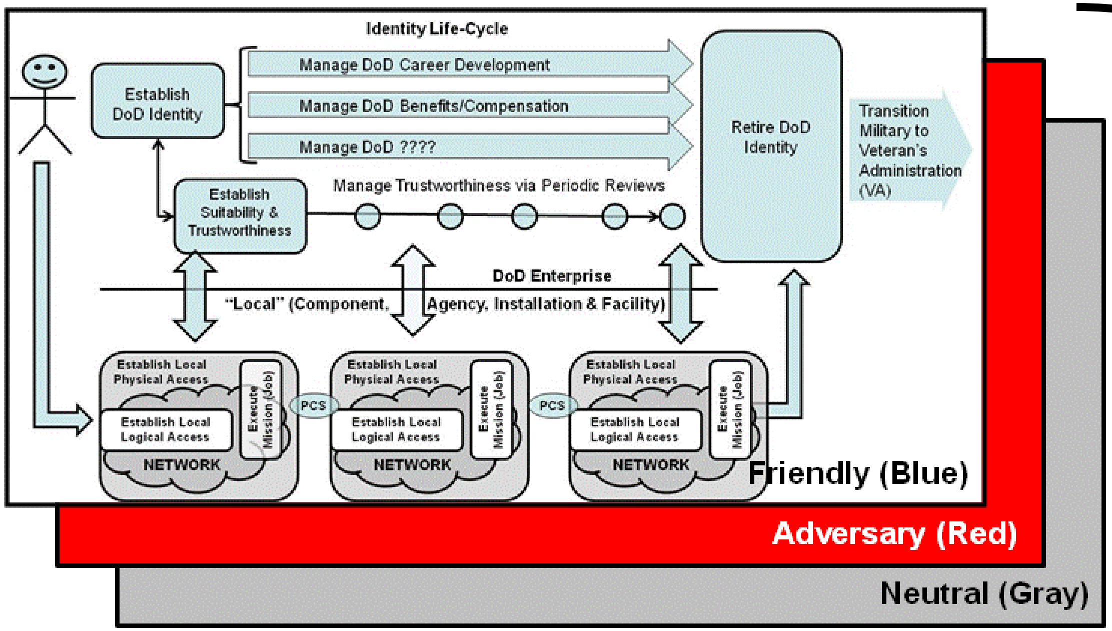
AUDIT
- Auditing & Reporting
- Reports Management
- Audit Trail

PERSON & NON-PERSON ENTITIES

EANCS

FICAM Service Area

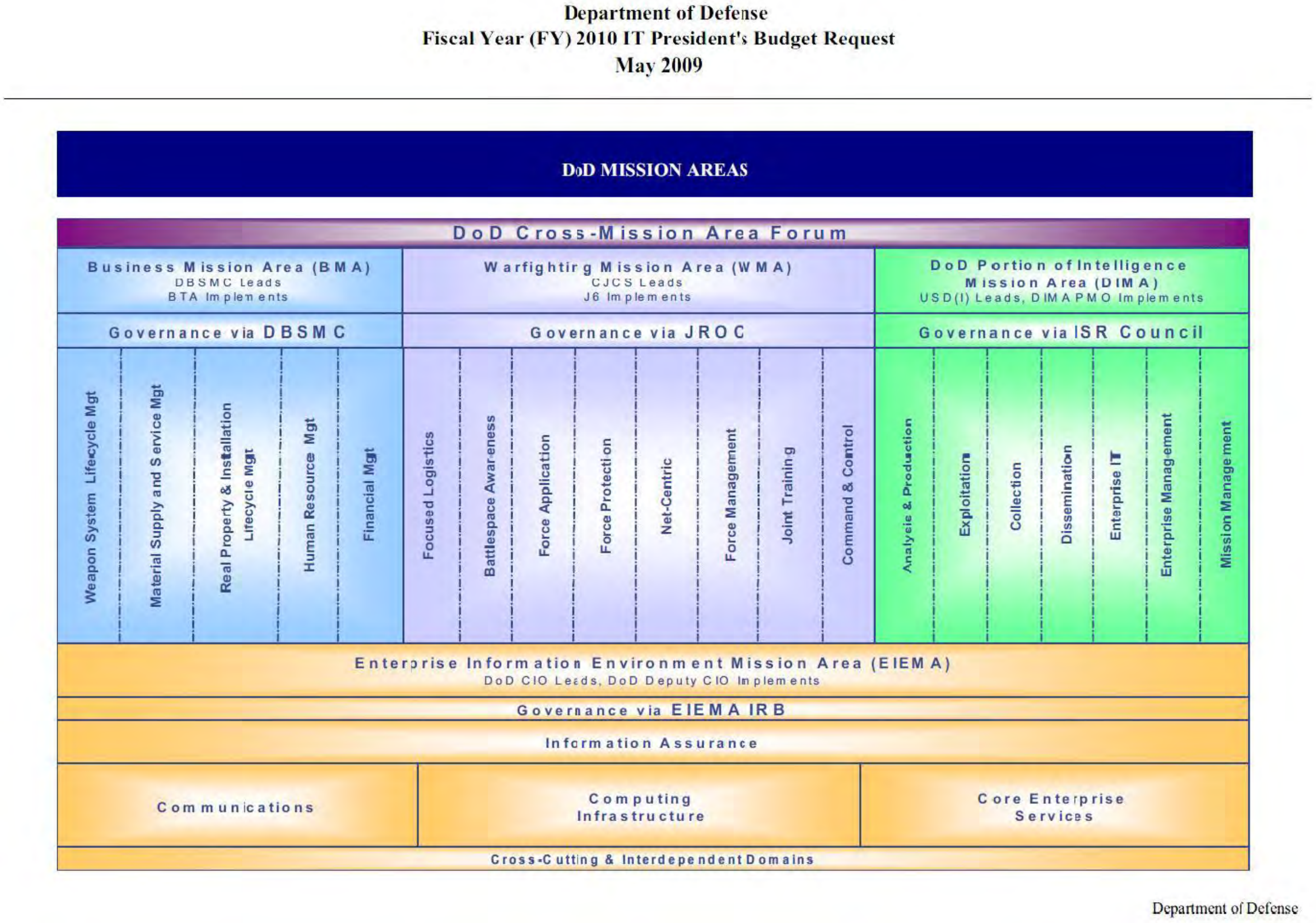
Notional Integrated IPvM Operational Capabilities


Identity Life-Cycle
Establish DoD Identity
Manage DoD Career Development
Manage DoD Benefits/Compensation
Manage DoD ????
Retire DoD Identity
Transition Military to Veteran's Administration (VA)
Establish Suitability & Trustworthiness
Manage Trustworthiness via Periodic Reviews
DoD Enterprise
"Local" (Component, Agency, Installation & Facility)
Establish Local Physical Access
Establish Local Logical Access
Execute Mission (Job)
NETWORK
PCS
Establish Local Physical Access
Establish Local Logical Access
Execute Mission (Job)
NETWORK
PCS
Establish Local Physical Access
Establish Local Logical Access
Execute Mission (Job)
NETWORK
Friendly (Blue)
Adversary (Red)
Neutral (Gray)

Each major Identity Population have a distinct Management & Technical Services Framework

- **Friendly Goals –** enabled trusted hiring, identity proofing & vetting for access control
- **Adversary Goals** – Find, Fix (Identity), Track & Act against Known or Suspected Threats to US National Security
- **Neutral Goals** – Identity proofing & vetting / Fix, track, other
- **Operational (aggregate) Goals** – Identity "superiority" capabilities that require integration of all of the above to achieve, e.g. *Force Protection; Cyber security; Personnel Recovery; other*

DoD Mission Areas



Department of Defense
Fiscal Year (FY) 2010 IT President's Budget Request
May 2009

DoD MISSION AREAS

DoD Cross-Mission Area Forum

Business Mission Area (BMA)
DBSMC Leads
BTA Implements

Governance via DBSMC

- Weapon System Lifecycle Mgt
- Material Supply and Service Mgt
- Real Property & Installation Lifecycle Mgt
- Human Resource Mgt
- Financial Mgt

Warfighting Mission Area (WMA)
CJCS Leads
J6 Implements

Governance via JROC

- Focused Logistics
- Battlespace Awareness
- Force Application
- Force Protection
- Net-Centric
- Force Management
- Joint Training
- Command & Control

DoD Portion of Intelligence Mission Area (DIMA)
USD(I) Leads, DIMA PMO Implements

Governance via ISR Council

- Analysis & Production
- Exploitation
- Collection
- Dissemination
- Enterprise IT
- Enterprise Management
- Mission Management

Enterprise Information Environment Mission Area (EIEMA)
DoD CIO Leads, DoD Deputy CIO Implements

Governance via EIEMA IRB

Information Assurance

Communications

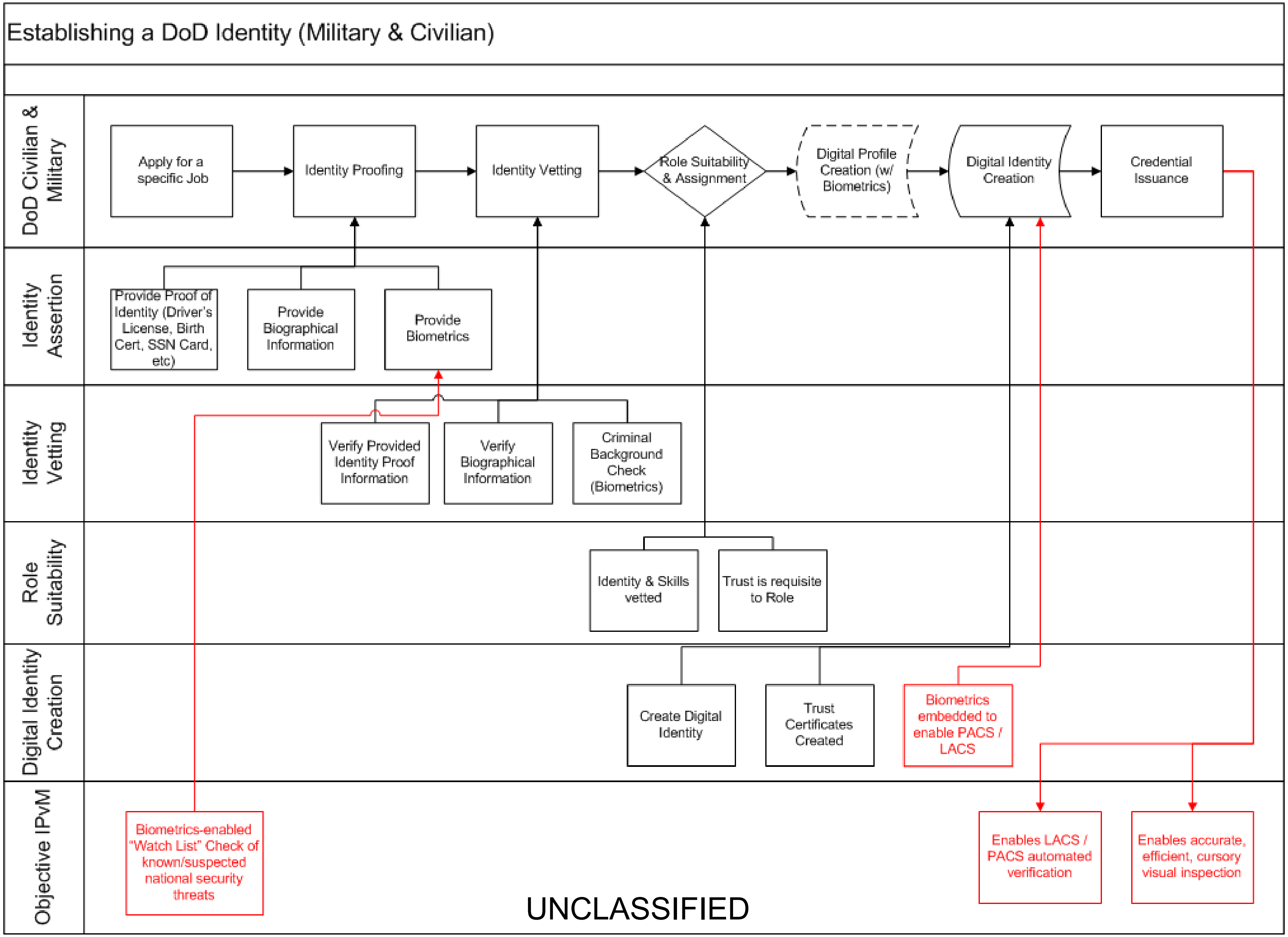
Computing Infrastructure

Core Enterprise Services

Cross-Cutting & Interdependent Domains

Department of Defense

"Hiring" Use Case Process Flow Diagram



Establishing a DoD Identity (Military & Civilian)

DoD Civilian & Military

Apply for a specific Job

Identity Proofing

Identity Vetting

Role Suitability & Assignment

Digital Profile Creation (w/ Biometrics)

Digital Identity Creation

Credential Issuance

Identity Assertion

Provide Proof of Identity (Driver's License, Birth Cert, SSN Card, etc)

Provide Biographical Information

Provide Biometrics

Identity Vetting

Verify Provided Identity Proof Information

Verify Biographical Information

Criminal Background Check (Biometrics)

Role Suitability

Identity & Skills vetted

Trust is requisite to Role

Digital Identity Creation

Create Digital Identity

Trust Certificates Created

Biometrics embedded to enable PACS / LACS

Objective IPvM

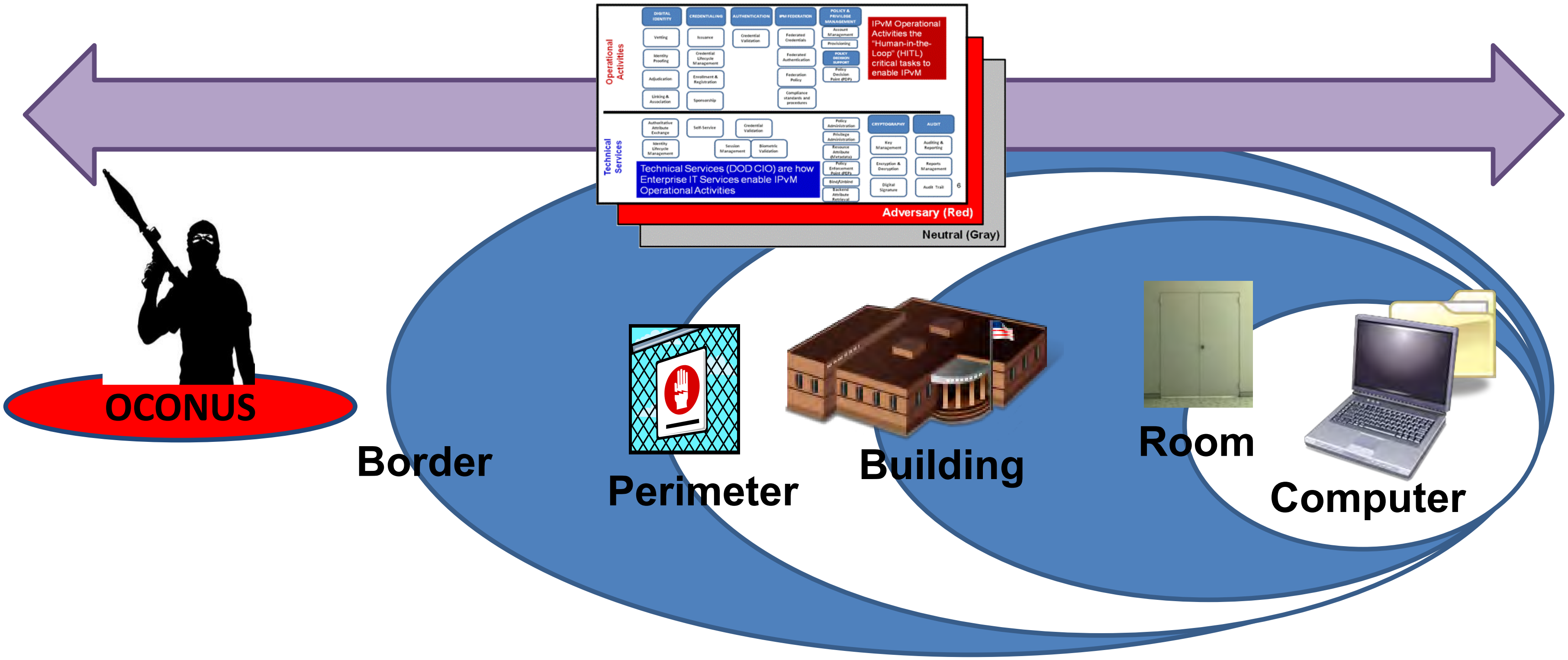
Biometrics-enabled "Watch List" Check of known/suspected national security threats

Enables LACS / PACS automated verification

Enables accurate, efficient, cursory visual inspection

UNCLASSIFIED

Notional IPvM *Defense in Depth* (1 of 2)



IPvM Operational Activities the "Human-in-the-Loop" (HITL) critical tasks to enable IPvM

Technical Services (DOD CIO) are how Enterprise IT Services enable IPvM Operational Activities

Systems of System (or integrated) IPvM Framework allows for assessing security requirements respective to risk to allow for more streamlined access control policies and processes "deeper" in the secure IPvM enclave.

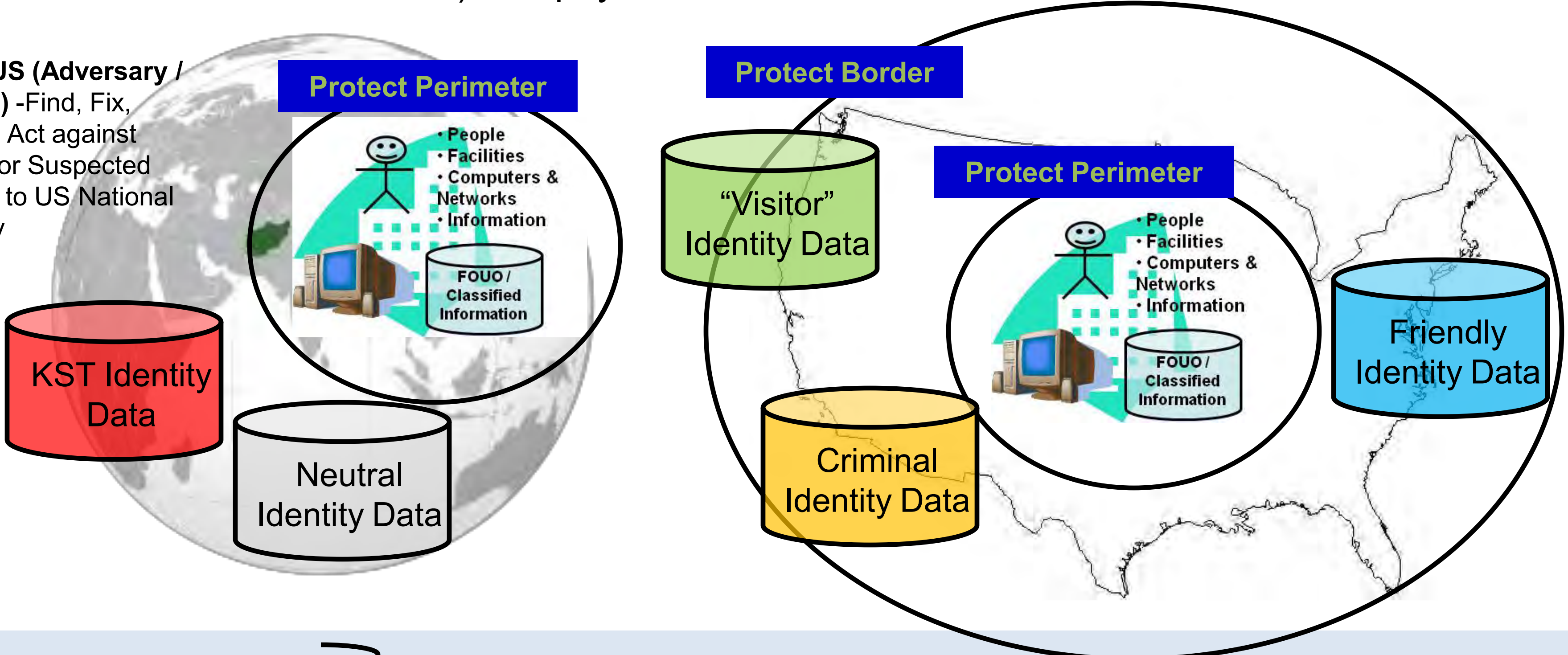
2011 DoD BIOMETRICS COLLABORATION FORUM

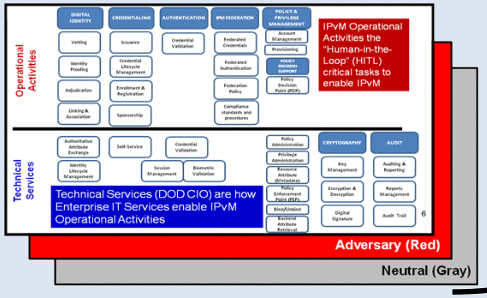
www.biometrics.dod.mil

Notional IPvM *Defense in Depth* (2 of 2)

Force Protection- The ability to prevent/mitigate adverse effects of attacks on personnel (combatant / non-combatant) and physical assets of the US, Allies & Friends

OCONUS (Adversary / Neutral) -Find, Fix, Track & Act against Known or Suspected Threats to US National Security





IPvM Operational Activities the "Human-in-the-Loop" (HITL) critical tasks to enable IPvM

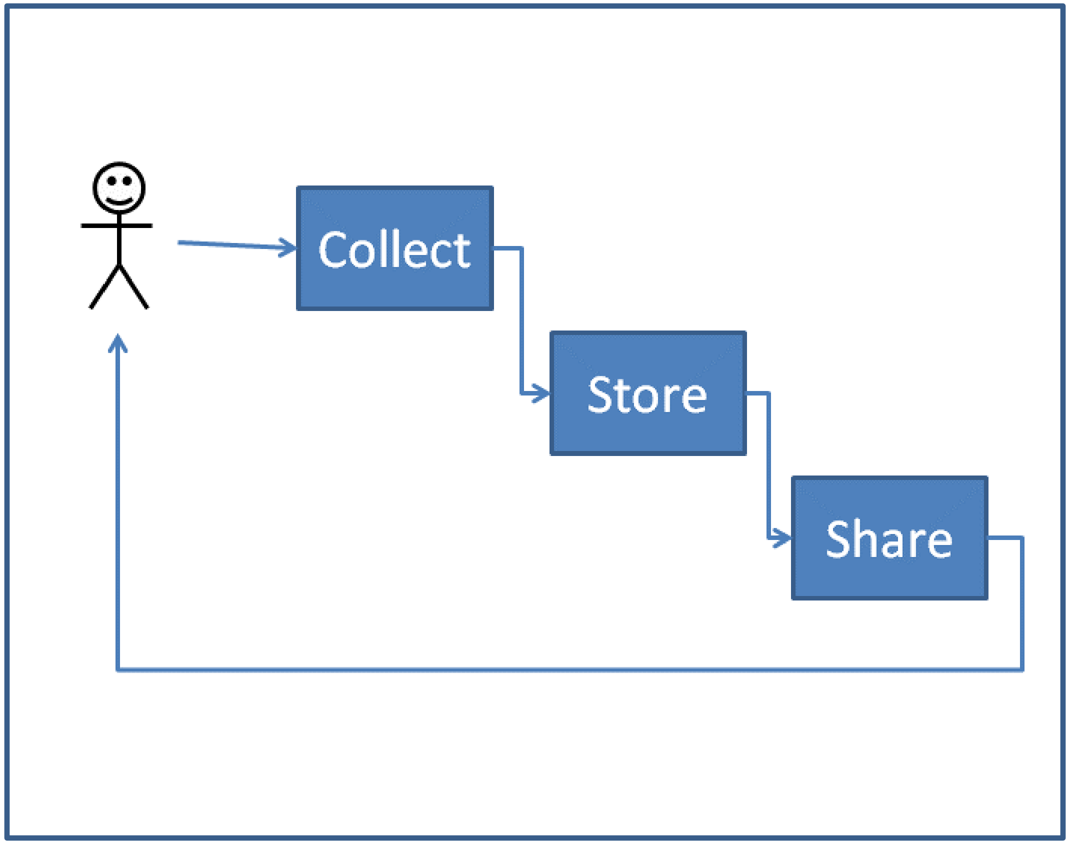
Technical Services (DOD CIO) are how Enterprise IT Services enable IPvM Operational Activities

- Manage Identity – across the full spectrum of IPvM Frameworks
- Manage Credentials – to align trusted roles to authorized access
- Manage Authentication – to ensure only authorized access
- Manage Privilege – manage life-cycle of aligned trusted roles & authorized access
- Manage IPvM Federation – Federate to enable IPvM Operational Goals and allow DoD business efficiencies

Privacy Compliance - more Systems Engineering than Policy Constraint

Friendly Biometric Systems require Privacy Impact Assessment:

- Collection
  - Signed Consent
  - Disclosure legal authority, handling (collect, store, share), purpose, etc.
- Storage & Share
  - System of Records Notice (SORN)



* The Privacy Act of 1974, E-Government Act of 2002 , other…

Findings DoD Identity Management Enterprise Services

- IPvM Policy & Guidance development & drafting
- **Identity proofing & vetting**
  - New hire
    - New – biometrics-enabled vetting against "Watch List" of known or suspected national security threats, i.e., checks that would result in actions, e.g., detain, deny access, etc.
  - Life-Cycle
- **Create *Digital Profile* to enable Human Resource Management (HRM)**
  - Digital Profile (Draft Definition) – electronic record with biographical, contextual & biometric information that describes a DoD Identity utilized to enable administrative management.
- **Create Digital Identity to enable Access Management**
  - Digital Identity – electronic representation of an individuals identity *to enable granting of privileges*
  - *Does this actually happen locally, is a certificate is all that is created at the enterprise level?*
- **Credential Issuance & Life-Cycle Management**

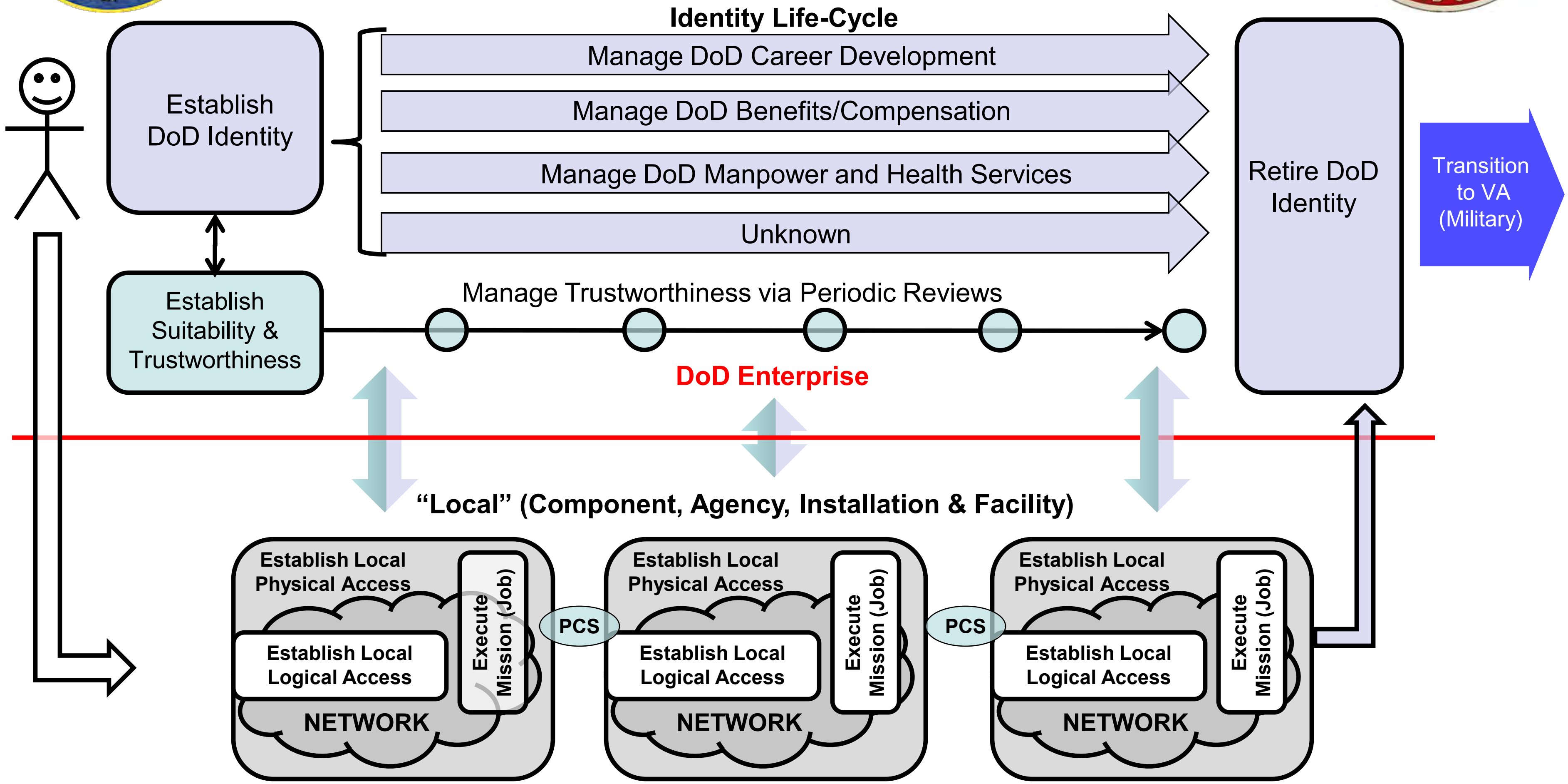
Note: DoD Services enable privilege management, the provisioning / deprovisioning of privileges and resulting management occurs "locally"

Findings DoD Identity Management & Privilege Management "Local" Services

- IPvM Policy & Guidance compliance & refinement
- Identity proofing & vetting
  - Visitors (short-term, limited access requirements) & tenants (TDY or PCS'd personnel and Contractors)
  - "Local Life-Cycle" – ensure access is granted for specific purpose and duration of need/requirement.
  - Really need to understand the policy driven use cases here…
- Leverage *Digital Profile* to enable Human Resource Management (HRM)
  - What are the policy/regulatory use case of PCS or TDY inprocessing????
- Leverage DoD Credential to Create Digital Identity to enable Access Management
  - Verify Trust
  - *Provision Access*
  - *Deprovision Access*
- Credential Issuance & Life-Cycle Management
  - Only applicable for "local" Credential requirements

Note: Local IPvM encompasses role assumption, perimeter access, facilities access, logical access and all associated "Local Life-Cycle" management requirements

Draft IPvM Conceptual "Cartoon" DoD Military and Civilian

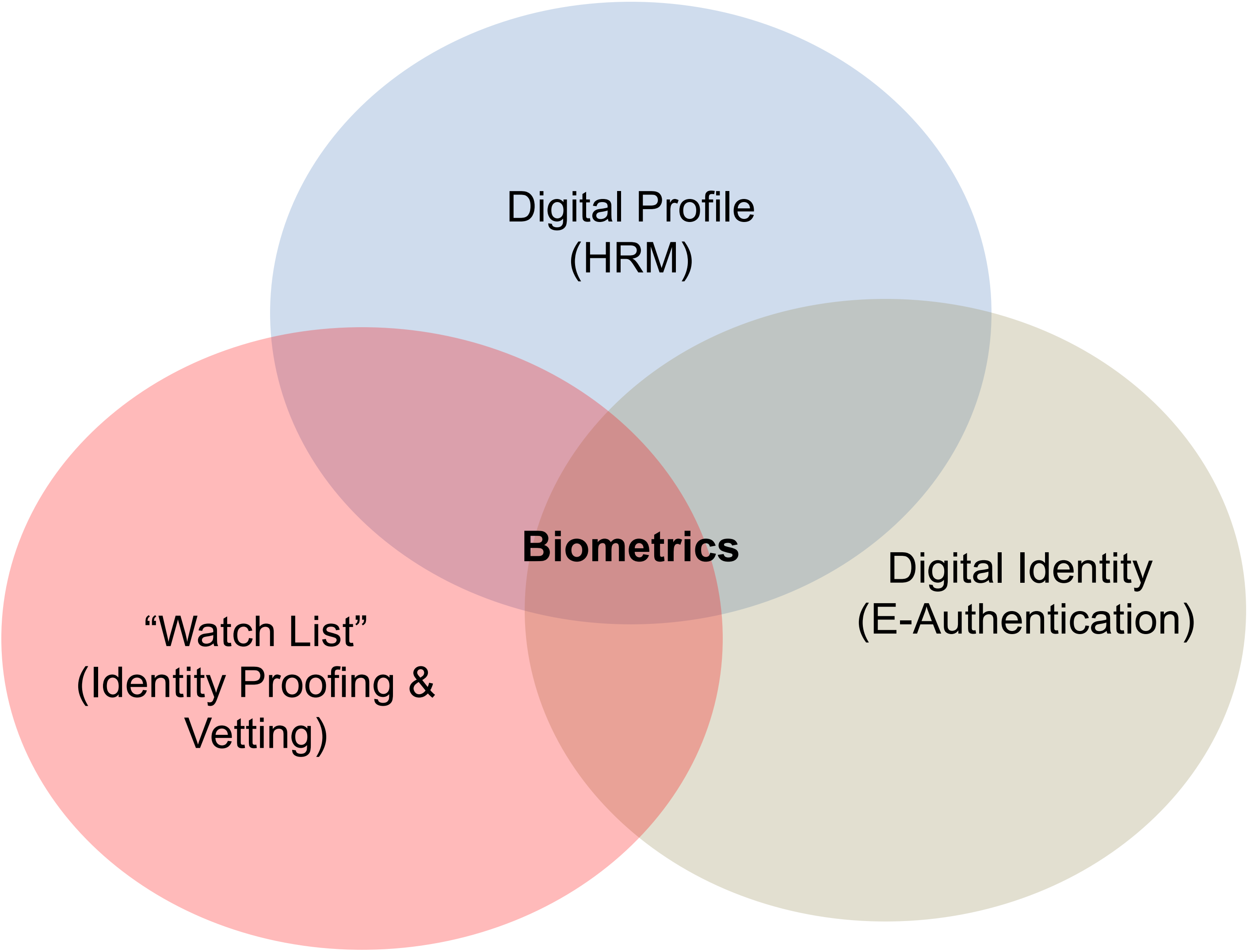

Identity Life-Cycle
Establish DoD Identity
Manage DoD Career Development
Manage DoD Benefits/Compensation
Manage DoD Manpower and Health Services
Unknown
Retire DoD Identity
Transition to VA (Military)
Establish Suitability & Trustworthiness
Manage Trustworthiness via Periodic Reviews
DoD Enterprise
"Local" (Component, Agency, Installation & Facility)
Establish Local Physical Access
Establish Local Logical Access
Execute Mission (Job)
NETWORK
PCS
Establish Local Physical Access
Establish Local Logical Access
Execute Mission (Job)
NETWORK
PCS
Establish Local Physical Access
Establish Local Logical Access
Execute Mission (Job)
NETWORK

USD Personnel & Readiness (P&R)
USD Intelligence (I)
Local commander/resource owner
Veterans Affairs (VA)

Terminology purposely abstracted up to very generic language & Concepts
IPvMWG will mature this "Cartoon" to a Model

Notional Friendly Force IPvM Biometric Enterprise Equities

- **Hiring**
  - Identity Proofing & Vetting
  - Credential Issuance (Digital Profile)
- **Biometrics-enabled Physical & Logical Access Control**
  - Identity Proofing & Vetting
- **Biometrics-enabled "Watch List"**
  - Hiring - Identity Proofing & Vetting
  - Identity Fixing
  - Identity Tracking
  - Authoritative Repository(s)
- **Personnel Recovery**
- Second Order Effects, i.e., if we can support all of the above, then we can
  - Humanitarian Assistance / Disaster Response
  - Personnel Accountability



Digital Profile
(HRM)

Biometrics

Digital Identity
(E-Authentication)

“Watch List”
(Identity Proofing & Vetting)

IPvMWG Contact Information

Co-Chairs, IPvMWG

Tim Fong
Deputy Director,
Identity Assurance & PKI Directorate
OASD (NII) / DASD, CI&IA
timothy.fong@osd.mil
703-604-3156

Arthur R. Friedman
Senior Strategist for Privilege Management
OASD (NII) / DASD, CI&IA
arfried@nsa.gov
240-373-1968

IPvMWG support:

Cynthia Odom (cynthia.odom.ctr@osd.mil) 703-604-3155
Peter Joukov (peter.joukov.ctr@osd.mil) 703-604-3154
Bruce Groskreutz (bagrosk@nsa.gov) 240-373-4303

IPvMWG Websites:

https://www.us.army.mil/suite/grouppage/103390
https://www.intelink.gov/sites/dodipmwg/default.aspx
Email peter.joukov.ctr@osd.mil to request access